第15卷 第3期 郑州工学院学报 Vol.15 No.3
1994年 9 月 Journal of Zhengzhou Institute of Technology Sep. 1994

矩阵上的线性递归序列*

王锦玲

(郑州工学院数理力学系)

摘 要: F_2上所有二阶矩阵构成一非交换环记为$M_2(F_2)$，简记为M，本文对M上的线性递归序列进行了初步探索，着重研究了这类序列与它的分量序列之间的联系，及它们的周期、复杂度之间的关系，同时也给出了其它一此较好性质。

关键词: 线性递归序列，生成多项式，周期，复杂度，矩阵

中图分类号: O151

1 概念及初步性质

设 M 是 F_2 上所有二阶矩阵构成的环，显然 M 是含有 16 个元素的非交换环。

定义：设 $A=(A_0, A_1, A_2, \cdots)$是 M 上的序列，若存在 M 中的元素 $D_0, D_1, \cdots, D_{n-1}$，使得 $\underline{A}$ 满足如下递归式

$$A_{k+n}=D_{n-1}A_{k+n-1}+D_{n-2}A_{k+n-2}+\cdots+D_0A_k \tag{1}$$

$k=0, 1, 2, \cdots$，则称序列 $\underline{A}$ 是 M 上 n 级线性递归序列，称$(A_{k+n-1}, A_{k+n-2}, \cdots A_k)$为序列 A 的一个状态。若取 $k=0$，则对应的状态称为初始状态。多项式$f(x)=IX^n+D_{n-1}X^{n-1}+\cdots+D_1X+D_0$称为序列 $\underline{A}$ 的特征多项式。

对于上述定义的序列有如下简单性质:

①上述定义的序列 $\underline{A}$ 一定是准周期的，即存在 l 和 k_0，使得对任 $k>k_0$，$A_{k+l}=A_k$

②若 D_0 是 M 中的可逆元，即是可逆矩阵，则序列 A 是周期的，即①中 $k_0=0$

③若设$A_k=\begin{bmatrix} a_k & \alpha_k \\ b_k & \beta_k \end{bmatrix}$，$\underline{a}$，$\underline{b}$，$\underline{\alpha}$，$\underline{\beta}$ 分别表示序列 $\underline{A}$ 的四个分量序列，则序列 $\underline{A}$ 的周期 P(A)等于四个分量序列的周期 $P(\underline{a})$，$P(\underline{b})$，$P(\underline{\alpha})$，$P(\underline{\beta})$的最小公倍数。

对于 A 的分量序列表示给出三种方法

① 递归式表示：设$D_k=\begin{bmatrix} c_k & d_k \\ e_k & f_k \end{bmatrix}$，由线性递归式（1），得

* 收稿日期: 1993-08-24

$$a_{k+n}=c_{n-1}a_{k+n-1}+c_{n-2}a_{k+n-2}+\cdots+c_0a_k+d_{n-1}b_{k+n-1}+d_{n-2}b_{k+n-2}+\cdots+d_0b_k \tag{2}$$

$$b_{k+n}=e_{n-1}a_{k+n-1}+e_{n-2}a_{k+n-2}+\cdots+e_0a_k+f_{n-1}b_{k+n-1}+f_{n-2}b_{k+n-2}+\cdots+f_0b_k \tag{3}$$

$k=0, 1, 2, \cdots$

在（2），（3）式中以 α_i 替代 a_i，β_i 替代 b_i 就得 A 的另外二个分量序列的递归式

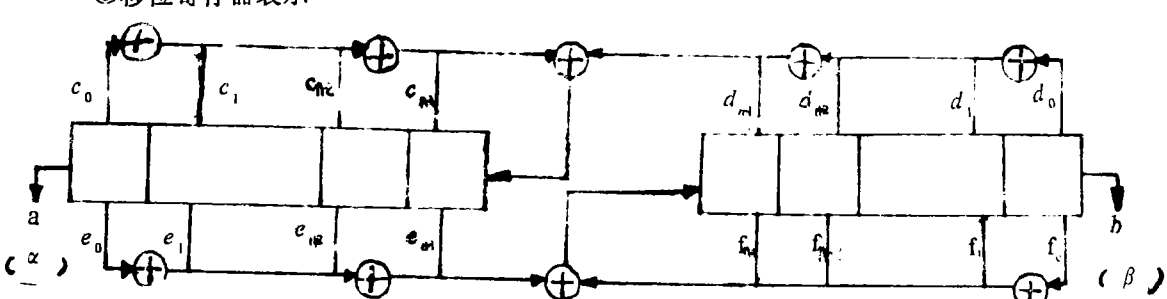
②矩阵式表示

$$\begin{bmatrix} a_{k+n} \\ b_{k+n} \\ a_{k+n-1} \\ b_{k+n-1} \\ \cdots \\ a_{k+2} \\ b_{k+2} \\ a_{k+1} \\ b_{k+1} \end{bmatrix} = \begin{bmatrix} c_{n-1} & d_{n-1} & c_{n-2} & d_{n-2} & \cdots\cdots & c_1 & d_1 & c_0 & d_0 \\ e_{n-1} & f_{n-1} & e_{n-2} & f_{n-2} & \cdots\cdots & e_1 & f_1 & e_0 & f_0 \\ 1 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots\cdots & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots\cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots\cdots & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a_{k+n-1} \\ b_{k+n-1} \\ a_{k+n-2} \\ b_{k+n-2} \\ \cdots \\ a_{k+1} \\ b_{k+1} \\ a_k \\ b_k \end{bmatrix} \tag{4}$$

$k=0, 1, 2, \cdots\cdots$

在（4）式中分别以 α_i，β_i 替代 a_i，b_i 则得另外二个分量序列的矩阵表示，（4）式中 $2n\times 2n$ 的矩阵可称作状态转移矩阵

③移位寄存器表示



2　分量序列的生成多项式

设 $a(t)=\sum_{i=0}^{\infty}a_it^i$，$b(t)=\sum_{i=0}^{\infty}b_it^i$，$c(t)=\sum_{i=0}^{n}c_it^{n-i}$，$d(t)=\sum_{i=0}^{n}d_it^{n-i}$，

$e(t)=\sum_{i=0}^{n}eit^{n-i}$，$f(t)=\sum_{i=0}^{n}fit^{n-i}$，其中 $c_n=d_n=e_n=f_n=1$，则由（2）式得

$$a(t)=\sum_{i=0}^{\infty}a_it^i=\sum_{i=0}^{n-1}a_it^i+\sum_{i=0}^{\infty}a_it^i$$

$$=\sum_{i=0}^{n-1}a_it^i+\sum_{i=n}^{\infty}(\sum_{j=0}^{n-1}c_ja_{i+j-n}+d_jb_{i+j-n})t^i$$

$$=\sum_{i=0}^{n-1}a_it^i+\sum_{j=0}^{n-1}(c_j\sum_{i=n}^{\infty}a_{i+j-n}t^i+d_j\sum_{i=n}^{\infty}b_{i+j-n}t^i)$$

$$=\sum_{i=0}^{n-1}a_it^i+c_0t^na(t)+c_1t^{n-1}(a_0+a(t))+\cdots+c_{n-1}t(a_0+a_1t+\cdots+a_{n-2}t^{n-2}$$

$$+a(t))+d_0t^nb(t)+d_1t^{n-1}(b_0+b(t))+\cdots+d_{n-1}t(b_0+\cdots+b_{n-2}t^{n-2}$$

$$+b(t))a(t)c(t)+b(t)(d(t)+1)=u(t) \tag{5}$$

其中$u(t)$是次数$\leqslant n-1$的多项式

同理利用（3）式有

$$a(t)(e(t)+1)+b(t)f(t)=v(t) \tag{6}$$

其中$v(t)$是次数$\leqslant n-1$的多项式

联立(5)和(6)解得

$$a(t)=\frac{\begin{bmatrix}u(t) & d(t)+1\\ v(t) & f(t)\end{bmatrix}}{\begin{bmatrix}c(t) & d(t)+1\\ e(t)+1 & f(t)\end{bmatrix}}\qquad b(t)=\frac{\begin{bmatrix}c(t) & u(t)\\ c(t)+1 & v(t)\end{bmatrix}}{\begin{bmatrix}c(t) & d(t)+1\\ e(t)+1 & f(t)\end{bmatrix}} \tag{7}$$

故序列a，b的生成多项式为

$$g(t)=\begin{vmatrix}c(t) & d(t)+1\\ e(t)+1 & f(t)\end{vmatrix}=c(t)f(t)+(e(t)+1)(f(t)+1) \tag{8}$$

同理可知，$\underline{\alpha}$，β的生成多项式也是(8)式中的$g(t)$，这样我们得到

定理 1 设 A 是由 (1) 式产生的 M 上 n 级线性递归序列，则序列 A 的四个 F_2 上的分量序列可由同一个 $2n$ 次多项式生成，且它们的生成多项式由（8）式给出

3 周期与复杂度

定理 2

①M 上 n 级线性递归序列的周期的上界是 4^n-1，分量序列的线性.复杂度的上界为 2n。

②设 A 是 M 上 n 级线性递归序列，则序列 $\underline{A}$ 的周期达到 4^n-1，当且仅当 A 是非零序列，且（8）式中分量序列的生成多项式 g(t)是 2n 次本原多项式

证: ①由（8）式中的 g(t)是四个分量序列的生成多项式，所以分量序列的线性复杂度不大于 2n，又每个分量序列的周期整除多项式 g(t)的周期 p(g(t))，所以序列 A 的周期也整除 p(g(t))，而 $p(g(t))<2^{2n}-1=4^n-1$，故序列 $\underline{A}$ 的周期不大于 4^n-1

②若 M 上 n 级线性递归序列 A 的周期是 4^n-1，则因为 A 的周期整除 p(g(t))，而 $p(g(t))<4^n-1$，所以 $p(g(t))=4^n-1=2^{2n}-1$，故 g(t)是 2n 次本原多项式。反之，若 A 非零，g(t) 是 2n 次本原多项式，则必有 A 中一条分量序列是 2n 级 m 序列，它的周期是 4^n-1，所以 $p(A)>4^n-1$，又由 1）知 $p(A)<4^n-1$，所以 $p(A)=4^n-1$

上述定理给出的二个上界是否能够达到，下述定理给予了回答。

定理3：在定理2中给出的二个上界通过适当选取 $D_i=\begin{pmatrix} c_i & d_i \\ e_i & f_i \end{pmatrix}$是可以达到的。

证：因为在 $F_2[t]$ 中总存在 $2n$ 次本原多项式，设 $W(t)=t^{2n}+W_{2n-1}t^{2n-1}+\cdots+W_1t+W_0$ 是 $F_2[x]$ 中的一个 $2n$ 次本原多项式，显然 $W_0=1$，令 $g(t)=W(t)$，得关于 c_i，d_i，e_i，f_i 的方程组（系数相等）

$$\begin{cases} d_0e_0+c_0f_0=1 \\ d_0e_1+d_1e_0+c_0f_1+c_1f_0=W_{2n-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ d_0e_{n-1}+d_1e_{n-2}+\cdots+d_{n-1}e_0+c_0f_{n-1}+c_1f_{n-2}+\cdots+c_{n-1}f_0=W_{n+1} \\ c_0+f_0+d_1e_{n-1}+\cdots+d_{n-1}e_1+c_1f_{n-1}+\cdots+c_{n-1}f_1=W_n \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ c_{n-2}+f_{n-2}+d_{n-1}e_{n-1}+c_{n-1}f_{n-1}=W_2 \\ e_{n-1}+f_{n-1}=W_1 \end{cases} \tag{9}$$

若令 $d_i=f_i=1$，则上述方程组变为关于 e_0，e_1，…，e_{n-1}，c_0，c_1，…，c_{n-1} 的线性方程组，系数矩阵如下：　　n 行　　n 行

$$\begin{matrix} \\ n\text{行} \\ \\ \\ \\ \\ n\text{行} \\ \\ \end{matrix}\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix}$$

n列　　n列

容易证上述矩阵是满秩的，所以关于 e_0，…，e_{n-1}，c_0…，c_{n-1} 的方程组是有解的，从而方程组（9）有解，故通过适当选取 D_i，$i=0$，1…，$n-1$，定理 2 中的二个上界都能达到

由定理2和定理3，我们知道 M 上 n 级线性递归序列的最长周期是 4^n-1，称这样的序列为 M 上 n 级 m^1- 序列

4 其它一些性质

性质1: M上n级 m^1-序列A，它们的所有非零分量序列是 F_2 上2n级m-序列，且两两平移等价。

证: 因为A中非零分量序列的生成多项式是2n次本原多项式g(t)，所以它们都是2n级m-序列，而由同一个本原多项式产生的序列必是平移等价。

针对定理2，考虑下述问题: 设B是M上的一个周期序列，且它的四个分量序列可由同一个2n次本原多项式生成，显然若 $B\neq 0$，则B的周期是 4^n-1，且B中的非零分量序列是两两平移等价，现在要问序列B是M上n级线性递归序列吗? 即是n级 m^1-序列吗?

性质2: 上述这样的序列B未必是n级 m^1-序列

证: 由2n次本原多项式生成的 F_2 上的序列必有连续2n-1个0出现，所以可以考虑下列序列。

连续n个零矩阵

$$B=(*,\ *,\ \cdots,\ *,\ \begin{pmatrix}0&0\\0&0\end{pmatrix},\ \cdots,\ \overbrace{\begin{pmatrix}0&0\\0&0\end{pmatrix}},\ *,\ \cdots\cdots)$$

则 B 显然不是 M 上 n 级线性递归序列，这里设 $B\neq 0$。

性质3: 设 $F(t)=It^n+D_{n-1}t^{n-1}+\cdots+D_1t+D_n$ 是 $M(t)$ 中的一个多项式，若有 M 上某 n 级 m^1- 序列以 $F(t)$ 为生成多项式，则由 $F(t)$ 产生的任一非零序列都是 M 上 n 级 m^1- 序列

证: 对应于 $F(t)$ 的(8)中的 $g(t)$ 是 $F(t)$ 所产生的序列的分量序列的生成多项式，由于有某 n 级 m^1- 序列以 $F(t)$ 为生成多项式，所以 $g(t)$ 必是 $2n$ 次本原多项式，从而由定理2知，由 $F(t)$ 产生的非零序列均是 n 级 m^1- 序列

称性质3中的 $F(t)$ 为 M 上 n 次拟本原多项式

性质4: M 上每个 n 次拟本原多项式能产生 4^n+2 个圈，其中 4^n+1 个 m^1- 序列形成的圈，另一个是零圈。

证: 设 $F(t)$ 是 n 次拟本原多项式，M 中共有16个元素，对 $F(t)$ 所产生的序列来说，共有 16^n 个可能的状态，而 $F(t)$ 所产生的每个非零序列的周期是 4^n-1，故有 4^n-1 个状态，另外 16^n 个状态中非零状态为 16^n-1，从而 $F(t)$ 能产生 $\dfrac{16^n-1}{4^n-1}=4^n+1$ 条两两不平移等价的非零序列，且是 n 级 m^1- 序列，故共有 4^n+1 个非零圈，其次 $F(t)$ 还产生一个零圈。

5 结束语

关于在通信中如何传输矩阵，我们可以把矩阵看作四个 F_2 上的元素 a_i，b_i，α_i，β_i 来传送，但这里也有一个问题，如果对其作四采样，由前面所述的性质知，这样排列的序列是易破的，不过我们可以对序列

$$a_0 b_0 \alpha_0 \beta_0 a_1 b_1 \alpha_1 \beta_1 \cdots\cdots$$

再作钟控或前馈等运算，就可以避免被采样所破。

有关 M 上线性递归序列，还有许多问题，可望进一步研究。

致谢周锦君教授戚文峰讲师热情指导和帮助。

参　考　文　献

1 Serge Lang, Algebra. Addison–Wesley, 1984

2 Rudolf Lidl, Finite Fields. Addison–Wesley 1983

3 万哲先. 代数和编码(修订版). 科学出版社. 1980

4 T. Beth, F.C. Piper, The Stop–and –Go Generfor. Proceedings of Eurocrypto. 84

5 W. Diffie, M. E. Hellman, New Directions in cryptography, IEEE Trans on IT–22, No, 6, 1976

6 王锦玲. 控制序列的构造与分析. 信息工程学院学报. 1993, 2

Linear Recurring Sequence in the Matrix

Wang Jingling

(Zhengzho Institute of Technology)

Abstract: The set of all 2× 2 Matrins over the finite field F_2 is written by $M_2(F_2)$, Simply M. In this paper, linear recurring sequences over M are discussed. Mainly study the relaitons among their subsequences, periods of subsequences and their complexities, Also other useful results are given.

Keywords: Linear recurring sequence, generating polynomial, period, Complexity, Matrices.